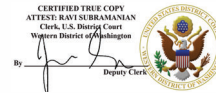


EXHIBIT A

UNITED STATES DISTRICT COURT

for the

Western District of Washington



In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 Business operating at 928 Thomas Road,
 Bellingham, WA 98226 et al.

Case No. MJ25-161

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachments A-1 and A-2, incorporated by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachments B-1 and B-2, incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

8 USC §§ 1324(a), 1324a;
 18 USC §§ 1001, 911, 1015(e),
 1546; 42 USC § 408(a)(7)(B)

Offense Description

Knowingly hiring unauthorized aliens; Intentional hiring unauthorized aliens; False & fictitious statements; False representation as U.S. citizen; False statement to obtain employment; Use of false identification documents; False use of Social Security number.

The application is based on these facts:

- ☒ See Affidavit of Special Agent [REDACTED], continued on the attached sheet.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means or ☐ telephonically recorded.

[REDACTED]
 Applicant's signature

HSI Special Agent [REDACTED]

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/25/25

[REDACTED]
 Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge

Printed name and title

1 investigation of transnational gangs. I am authorized to investigate and enforce
2 violations of federal criminal statutes, including those in Titles 8, 18, and 21 of the
3 United States Code.

4 3. My experience as a federal law enforcement officer and criminal
5 investigator includes the investigation and prosecution of violations of criminal laws
6 relating to unlawful entry, employment, and physical presence in the United States. My
7 current duties include conducting criminal investigations of violations of Federal Statutes
8 and administrative violations of the INA and Title 18 of the United States Code. As part
9 of these duties, I have become involved in the investigation of suspected violations of
10 Title 8, United States Code, Section 1324(a), Unlawful Employment of Aliens. Through
11 formal and on the job training, I am experienced in crimes involving the unlawful
12 employment of aliens.

13 4. I have participated in the execution of numerous search warrants for
14 documents and other evidence, including computers and electronic media.

15 5. I make this affidavit in support of an application under Rule 41 of the Federal
16 Rules of Criminal Procedure for a warrant to search the following premises and persons:

17 a. The business located at 928 Thomas Road, Bellingham, WA 98226,
18 and its curtilage and outbuildings, appurtenances, and attached and detached garages and
19 company vehicles and trailers located on such curtilage, including any and all parking
20 lots, further described in Attachment A-1 (sometimes referred to as the "business"),
21 incorporated herein by reference.

22 b. Fifty-six individuals, further described in Attachment A-2,
23 incorporated herein by reference.

24 6. This affidavit sets forth facts establishing probable cause to believe that
25 Frog Hill Roofing LLC, d/b/a, Mt. Baker Roofing (hereinafter "Mt. Baker Roofing") is
26 unlawfully employing aliens without legal work authorization in violation of federal
27 criminal law. In addition, this affidavit establishes that there is probable cause to believe

1 that the fifty-six individuals identified in Attachment A-2 fraudulently represented their
 2 immigration status and submitted false documents and/or information in order to seek
 3 employment. I seek authorization to seize the items specified in Attachments B-1 (for the
 4 business) and Attachment B-2 (for the individuals).

5 7. The information in this affidavit is based on the investigation I have
 6 conducted in this case, my conversations with other law enforcement officers who have
 7 engaged in various aspects of this investigation, and my review of reports written by
 8 other law enforcement officers involved in this investigation. Because this Affidavit is
 9 being submitted for the limited purpose of securing the requested warrant, I have not
 10 included each and every fact known to me concerning this investigation. I have set forth
 11 only those facts that I believe are relevant to a determination of probable cause to support
 12 the issuance of the requested warrant. When the statements of others are set forth in this
 13 Affidavit, they are set forth in substance and in part. Times listed in the Affidavit are
 14 approximate.

15 **RELEVANT LAW AND ADDITIONAL KNOWLEDGE OF AFFIANT**

16
 17 8. Section 274A of the Immigration and Reform Act of 1986 (IRCA) contains
 18 provisions that require all employers to verify the employment eligibility of all new
 19 employees hired after November 6, 1986. The Form I-9 (Employment Eligibility
 20 Verification), hereinafter referred to as Form I-9, was developed for verifying that
 21 persons are eligible to work in the United States. Employers must ensure that a Form I-9
 22 is completed every time a person is hired to perform labor or services in return for wages
 23 or other remuneration. The Form I-9 is comprised of three sections.

24 9. Section 1 is to be completed by the employee at the time of hire. This
 25 section contains the fields of name, address, date of birth, Social Security Number, and
 26 the attestation of the employee as to their immigration status in the United States.

27 10. Section 2 is to be completed by the employer and consists of three separate
 columns for List A (Identity and Employment Eligibility), List B (Identity only), and List

C (Employment Eligibility only) documents. In order for an employee to be deemed eligible to work, the employer must examine one document from List A, or one document from List B and one document from List C. Examples of List A documents include United States Passports, Certificates of Naturalization, Forms I-551 (sometimes referred to as Permanent Resident cards or “green cards”), or Employment Authorization cards. Examples of List B documents include driver’s licenses and voter registration cards. Examples of List C documents include Social Security cards and birth certificates. The employer is required to examine original documents presented by an employee and then complete this section of the I-9 form within three days of employment beginning.

11. Section 3 of the I-9 Form, referred to as Supplement B, is completed by the employer under circumstances where the law requires an employee’s status to be reverified, when an employee is terminated and rehired within three years of the date the original Form I-9 was completed, or when an employee has changed his or her name.

12. Employers must retain all I-9 forms for three years after the date a person’s employment begins or one year after the person’s employment is terminated, whichever is later.

13. E-Verify is an internet-based system that compares information entered by an employer from an employee's Form I-9 to records available to the U.S. Department of Homeland Security and the Social Security Administration, in order to allow the employer to verify the accuracy of the information submitted. The system is free to use by employers but not mandated by federal law.

14. Any person who, during any 12-month period, knowingly hires for employment at least 10 individuals with actual knowledge that the individuals are unauthorized aliens is subject to criminal penalties under Title 8, United States Code, Section 1324(a)(3)(A) & (B).

15. Intentional hiring of unauthorized aliens is also a violation of Title 8, United States Code, Section 1324a. A person or entity who engages in a pattern and practice of violating this provision is subject to imprisonment and fines.

16. In addition, a person or entity who willfully submits a Form I-9 to the government containing materially false, fictitious, or fraudulent statements is subject to criminal penalties under Title 18, United States Code, Section 1001.

17. A person who falsely and willfully represents themselves as a United States citizen is subject to criminal penalties under Title 18, United States Code, Section 911.

18. A person who knowingly makes a false statement that they are a citizen or national of the United States in order to engage unlawfully in employment in the United States is subject to criminal penalties under Title 18, United States Code, Section 1015(e).

19. It is a crime for an individual to use a Social Security number not assigned to them, with the intent to deceive, in order to obtain anything of value, under Title 42, United States Code, Section 408(a)(7)(B).

20. Finally, a person who uses an identification document in connection with completing a Form I-9 knowing that the identification document was not issued lawfully for the use by that person is subject to criminal penalties under Title 18, United States Code, Section 1546(b).

21. As set forth in the remainder of this Affidavit, there is probable cause to believe that a search of the business and the individuals listed in Attachments A will reveal evidence of the foregoing crimes.

PROBABLE CAUSE

A. Identification of Mt. Baker Roofing

22. On January 27, 2025, HSI received a tip that Mt. Baker Roofing was employing unauthorized aliens. Mt. Baker Roofing is a roofing company located at 928 Thomas Road, Bellingham, WA 98226.¹

¹ According to the State of Washington's Department of Labor & Industries, Mt. Baker Roofing's legal business name is Frog Hill Roofing LLC.

23. On February 26, 2025, HSI personnel served Mt. Baker Roofing with a Notice of Inspection requiring the company to produce their Forms I-9 within three business days. On March 4, 2025, HSI personnel returned to Mt. Baker Roofing and were provided with a binder that consisted of eighty-four Forms I-9 and supporting documentation that purportedly pertained to all current and former employees of the business within the past twelve months. HSI personnel asked the owner of the company whether he used E-Verify. The owner responded that he does not because it is not required and many of his competitors do not use it.

24. HSI personnel thereafter reviewed the material. As documented below, HSI personnel have identified 56 instances in which a fraudulent Form I-551, *i.e.*, a green card, was submitted or otherwise false attestations that employees were United States citizens, when in fact they were not.

B. Fraudulent Green Cards

25. Our review identified fifty-four instances in which fraudulent green cards were submitted. United States Citizenship and Immigration Services (USCIS) issues a green card to an individual when they become a lawful permanent resident of the United States. Green cards display the alien registration number (A-number) of the individual. An A-number is a unique number assigned to each alien who is processed by the United States. When an individual obtains a green card, multiple immigration records are generated to reflect the event.

26. HSI personnel determined that the cards were fake by querying immigration databases. The queries showed that the A-numbers listed on the cards did not match the names of the persons listed on the cards. In addition, some of the cards showed obvious signs of being fraudulent. For example, the font on some of the cards was inconsistent. In other instances, smudges were visible that appeared designed to obstruct the photo or some identifying information on the card. In addition, some of the cards displayed inconsistent holograms or authentication features, inconsistent spacing between names, and poor-quality photographs of the individual.

27. I know from my training and experience that one of the more recent versions of the green card was issued by U.S. Citizenship and Immigration Services in May 2017. This version includes three transparent stars, holographic features, as well as tactile features on the front of the card. Before May 2017, the previous version of the green card was introduced in May 2010. This laser-engraved version includes a holographic feature over the right side of the photo zone and an eagle's head in the upper left of the card composed of color-shifting ink. When the counterfeit green cards submitted by employees at Mt. Baker Roofing are compared to that of an authentic green card, noticeable discrepancies are apparent.

28. The following is an example of a legitimate green card submitted by an employee of Mt. Baker Roofing:



Legitimate LPR card (front) submitted by employee of Mt. Baker Roofing²

² Some personally identifiable information has been redacted for privacy reasons.

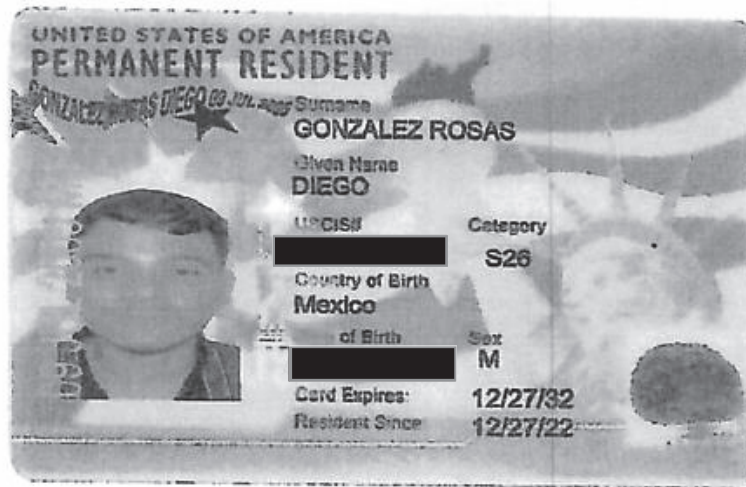
29. In contrast, the following four green cards differ in notable ways:
- 30.



This green card contained the following issues: name and date of birth located at the top left is not in a bold font and does not cover the middle star; USCIS# and date of birth does not align with the other biographical information; Category X6 is not a legitimate Immigrant Class of Admission; biographical information is displayed in different fonts; photograph should contain a white background surrounded by a multiline border; date of birth design and font to the left of the photograph is not consistent with the multiline border; the Statue of Liberty hologram to the right of the subject's photograph is barely visible; and the width of the bottom strip is not true to size.³

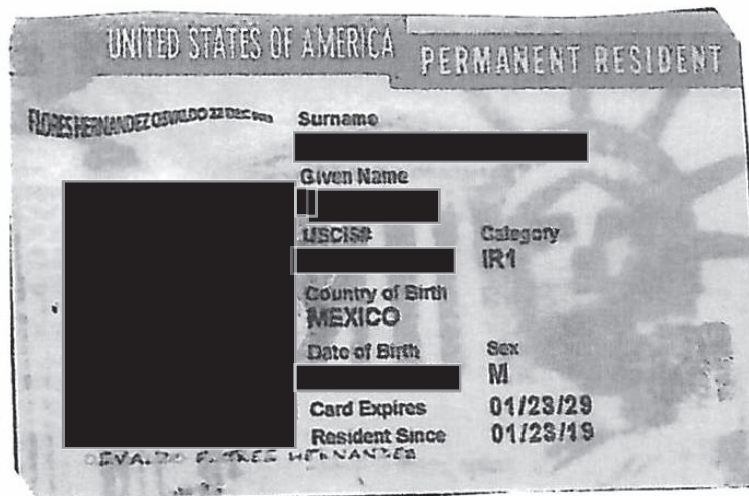
³ The copies of the identification documents that the business provided in connection with the I-9 audit were in black-and-white. Most of the copies were of poor quality, especially those determined to be fraudulent.

31.



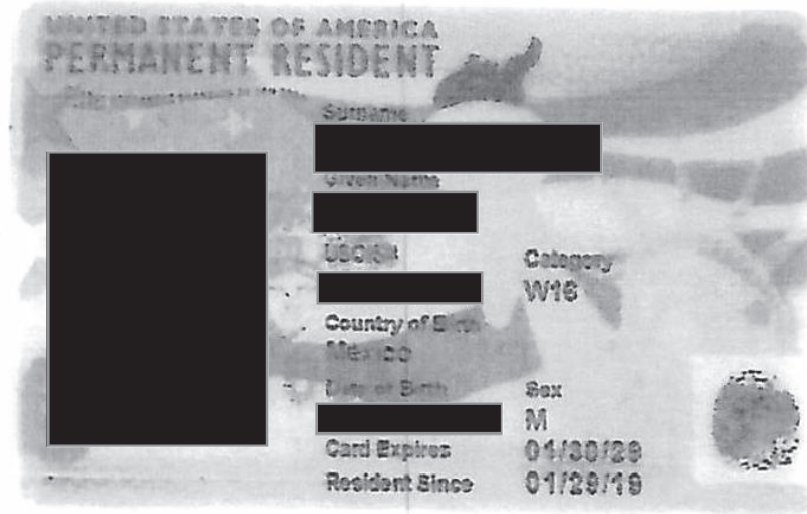
This green card contained the following issues: biographical data are not aligned; photograph should contain a white background surrounded by a multiline border; the photograph appears to be stretched and is not clear; the Statue of Liberty hologram to the right of the photograph is barely visible; and the Statue of Liberty located at the right appears deformed.

32.



This green card contained the following issues: name and date of birth located at the top left is in the incorrect font and not spaced appropriately; surname is incorrectly spaced; font of biographical data is inconsistent; and it appears the eagle's head at the top left and subject's fingerprint at the bottom right are nonexistent.

33.



This card contained the following issues: three transparent stars located at the top left are not true to size and both Statue of Liberty holographic features appear to be nontransparent.

34. HSI personnel undertook an attempt to determine the true identities of the persons associated with the 54 fraudulent green cards. Specifically, personnel queried databases to look for the names, dates of birth, and photographs displayed on the fraudulent cards. The personnel concluded as follows:

35. One of the cards submitted contained the name [REDACTED] and a particular date of birth. I searched government databases and identified an individual named [REDACTED] who has the same birth date and resembles the photograph on the fraudulent card. The address on his state-issued driver's license also matches what was provided on the Form I-9.

36. One of the cards submitted contained the name Jorge Luis ARROYO-Vilchez and a particular date of birth. I searched government databases and identified an individual named Jorge Luis ARROYO-Vilchez who has the same birth date and resembles the photograph on the fraudulent card. The address on his state-issued driver's license also matches what was provided on the Form I-9.

37. One of the cards submitted contained the name Heriberto AYALA-Gonzalez and a particular date of birth. I searched government databases and identified an individual named Heriberto AYALA-Gonzalez who has the same birth date and resembles the photograph on the fraudulent card. The address on his state-issued driver's license also matches what was provided on the Form I-9.

38. One of the cards submitted contained the name [REDACTED] and a particular date of birth. I searched government databases and identified an individual named [REDACTED] who has the same date of birth and resembles the photograph on the fraudulent card. The address on his state-issued driver's license also matches what was provided on the Form I-9.

39. One of the cards submitted contained the name Marco Antonio CISNEROS-Palomino and a particular date of birth. I searched federal government databases, found a Mexican passport, and identified an individual named Marco Antonio CISNEROS-Palomino who has the same date of birth and resembles the photograph on the fraudulent card.

40. One of the cards submitted contained the name [REDACTED] and a particular date of birth. I searched government databases and identified an individual named [REDACTED] who has the same date of birth and resembles the photograph on the fraudulent card. While the trailer number (*i.e.*, unit number) is different on his state-issued driver's license from what is shown on the Form I-9, the address is the same.

41. One of the cards submitted contained the name [REDACTED] and a particular date of birth. I searched government databases and identified an individual named [REDACTED] who has the same date of birth and resembles the photograph on the fraudulent card.

42. One of the cards submitted contained the name [REDACTED] and a particular date of birth. I searched government databases and identified

1 an individual named [REDACTED] who has the same date of birth and
2 resembles the photograph on the fraudulent card. The address on his state-issued driver's
3 license, [REDACTED] is very similar to what was provided on the Form
4 I-9, [REDACTED]. Additionally, while the fraudulent card and the
5 driver's license shows FLORES with an "s", the Form I-9 shows FLOREZ with a "z".

6 43. One of the cards submitted contained the name [REDACTED]
7 [REDACTED] and a particular date of birth. I searched government databases and identified
8 an individual named [REDACTED] who has the same birth date and
9 resembles the photograph on the fraudulent card. Even though the first names are one
10 letter off, I believe this to be the same person because the signature on the Form I-9
11 shows a first name of "[REDACTED]".

12 44. One of the cards submitted contained the name [REDACTED] and a
13 particular date of birth. I searched government databases and identified an individual
14 named [REDACTED] who has the same date of birth and resembles the
15 photograph on the fraudulent card. The address on his state-issued driver's license also
16 matches what was provided on the Form I-9.

17 45. One of the cards submitted contained the name Hugo Alfredo FUERTE-
18 Nunez and a particular date of birth. I searched government databases and identified an
19 individual named Hugo Alfredo FUERTE-Nunez who has the same date of birth and
20 resembles the photograph on the fraudulent card. The address on his state-issued driver's
21 license also matches what was provided on the Form I-9.

22 46. One of the cards submitted contained the name [REDACTED] and a
23 particular date of birth. The Form I-9 contained the name, [REDACTED]
24 [REDACTED]. I searched government databases and identified an individual named [REDACTED]
25 [REDACTED] who has the same date of birth and resembles the photograph
26 on the fraudulent card. The address on his state-issued driver's license also matches what
27 was provided on the Form I-9.

1 47. One of the cards submitted contained the name Ezequiel GOMEZ and a
2 particular date of birth. I searched government databases and identified an individual
3 named Ezequiel GOMEZ-Cruz who has the same date of birth and resembles the
4 photograph on the fraudulent card. The address on his state-issued driver's license also
5 matches what was provided on the Form I-9.

6 48. One of the cards submitted contained the name Santos GONZALEZ-
7 Feliciano and a particular date of birth. I searched government databases and identified
8 an individual named Santos GONZALEZ-Feliciano who has the same date of birth;
9 however, no photograph exists under that driver's license. Further record checks in
10 federal databases revealed his previous immigration history and a 2022 photograph that
11 resembled the individual depicted on the fraudulent card.

12 49. One of the cards submitted contained the name, Diego GONZALEZ-Rosas,
13 and a particular date of birth. I searched government databases and identified an
14 individual named Diego GONZALEZ-Rosas who has the same date of birth and
15 resembles the photograph on the fraudulent card. The address on his state-issued driver's
16 license also matches what was provided on the Form I-9.

17 50. One of the cards submitted contained the name Frank Brayan
18 GUTIERREZ-Gutierrez and a particular date of birth. I searched government databases
19 and identified an individual named Frank Brayan GUTIERREZ-Gutierrez who has the
20 same date of birth and resembles the photograph on the fraudulent card.

21 51. One of the cards submitted contained the name Iran HURTADO-Cancino
22 and a particular date of birth. I searched government databases and identified an
23 individual named Iran HURTADO-Cancino who has the same date of birth and
24 resembles the photograph on the fraudulent card. The address on his state-issued driver's
25 license also matches what was provided on the Form I-9.

26 52. One of the cards submitted contained the name Alejandro JUAREZ-
27 Galindo and a particular date of birth. I searched government databases and identified an

1 individual named Alejandro JUAREZ-Galindo who has a similar date of birth, which is
2 three days different; however, the photograph associated with his state-issued driver's
3 license resembles the photograph on the fraudulent card. In my experience, fraudulent
4 documents often will not have the precisely accurate biographical data as the subject,
5 especially for those individuals attempting to conceal their criminal or immigration
6 history.

7 53. One of the cards submitted contained the name [REDACTED]
8 and a particular date of birth. I searched government databases and identified an
9 individual named [REDACTED] who has the same date of birth and
10 resembles the photograph on the fraudulent card.

11 54. One of the cards submitted contained the name [REDACTED]
12 [REDACTED] and a particular date of birth. I searched government databases and identified an
13 individual named [REDACTED] who has the same date of birth and
14 resembles the photograph on the fraudulent card.

15 55. One of the cards submitted contained the name Joaquin JUAREZ-Ortiz and
16 a particular date of birth. I searched government databases and identified an individual
17 named Joaquin JUAREZ-Ortiz who has the same date of birth. Due to the poor image
18 quality on the fraudulent document, I am unable to determine if the photograph on the
19 fraudulent card matches the one on his state-issued driver's license; however, the address
20 listed on both the driver's license and the Form I-9 are the same, along with the same
21 name and date of birth. In my training and experience, the use of photograph
22 substitutions and poor-quality photographs are characteristics of fraudulent documents
23 and ones not used on official government identifications.

24 56. One of the cards submitted contained the name Victor LOPEZ-Gonzalez
25 and a particular date of birth. I searched government databases and identified an
26 individual named Victor LOPEZ-Gonzalez who has the same date of birth. Again, due to
27 the poor image quality on the fraudulent document, I am unable to determine if the

1 photograph on the fraudulent card matches the one on the driver's license; however, the
2 address listed on both his state-issued driver's license and the Form I-9 are the same,
3 along with the same name and date of birth.

4 57. One of the cards submitted contained the name Alberino LOPEZ-Cruz and
5 a particular date of birth. I searched government databases and identified an individual
6 named Alberino LOPEZ-Cruz, whose photograph resembles the photograph on the
7 fraudulent card. However, the date of birth on the fraudulent card is [REDACTED]
8 while the date of birth listed on his state-issued driver's license is [REDACTED]. The
9 date of birth on the subject's criminal history is also listed as [REDACTED].

10 However, the address listed on the Form I-9 and the one listed on his license is the same.
11 As previously mentioned, it is not uncommon to see different dates of birth on fraudulent
12 documents for those with immigration and criminal history.

13 58. One of the cards submitted contained the name Omar MARILES-Valencia
14 and a particular date of birth. I searched government databases and identified an
15 individual named Omar MARILES-Valencia who has the same date of birth and
16 resembles the photograph on the fraudulent card.

17 59. One of the cards submitted contained the name Elder MANCIA and a
18 particular date of birth. I searched government databases and identified an individual
19 named Elder Edgardo MANCIA-Ramirez who has the same date of birth. Due to the
20 poor image quality on the fraudulent document, I am unable to determine if the
21 photograph on the fraudulent document matches the one on his state-issued driver's
22 license.

23 60. One of the cards submitted contained the name Angel MARTINEZ-
24 Gonzalez and a particular date of birth. I searched government databases and identified
25 an individual named Angel MARTINEZ-Gonzalez who has the same date of birth and
26 resembles the photograph on the fraudulent card. The address on his state-issued driver's
27 license also matches what was provided on the Form I-9.

1 61. One of the cards submitted contained the name Luis Mario MARTINEZ-
2 Ortela and a particular date of birth. I searched government databases and identified an
3 individual named Luis Mario MARTINEZ-Ortela who has the same date of birth and
4 resembles the photograph on the fraudulent card.

5 62. One of the cards submitted contained the name Rogelio MARTINEZ-
6 Ortela and a particular date of birth. I searched government databases and identified an
7 individual named Rogelio MARTINEZ-Ortela who has the same date of birth. Again,
8 due to the poor image quality on the fraudulent document, I am unable to determine if the
9 photograph on the fraudulent card matches the one on his state-issued driver's license.

10 63. One of the cards submitted contained the name Jose Manuel MATEO and a
11 particular date of birth. I searched government databases and identified an individual
12 named Jose Manuel MATEO who has the same date of birth and resembles the
13 photograph on the fraudulent card. The address on his state-issued driver's license also
14 matches what was provided on the Form I-9.

15 64. One of the cards submitted contained the name Cristobal MORALES-Ortiz
16 and a particular date of birth. I searched government databases and identified an
17 individual named Cristobal MORALES-Ortiz who has the same date of birth and
18 resembles the photograph on the fraudulent card. The address on his state-issued driver's
19 license also matches what was provided on the Form I-9.

20 65. One of the cards submitted contained the name Jesus Abelardo
21 MORELOS-Cuevas and a particular date of birth. I searched government databases and
22 identified an individual named Jesus Abelardo MORELOS-Cuevas who has the same
23 date of birth and resembles the photograph on the fraudulent card. The address on his
24 state-issued driver's license also matches what was provided on the Form I-9.

25 66. One of the cards submitted contained the name [REDACTED]
26 [REDACTED] and a particular date of birth. I searched government databases and identified an
27 individual named [REDACTED] who has the same date of birth and

1 resembles the photograph on the fraudulent card. The address on his state-issued driver's
2 license also matches what was provided on the Form I-9.

3 67. One of the cards submitted contained the name [REDACTED] and
4 a particular date of birth. I searched government databases and identified an individual
5 named [REDACTED] who has the same date of birth and resembles the
6 photograph on the fraudulent card. The address on his state-issued driver's license also
7 matches what was provided on the Form I-9.

8 68. One of the cards submitted contained the name Edgar OLMOS-Vazquez
9 and a particular date of birth. I searched government databases and identified an
10 individual named Edgar OLMOS-Vazquez who has the same date of birth and resembles
11 the photograph on the fraudulent card. The address on his state-issued driver's license
12 also matches what was provided on the Form I-9.

13 69. One of the cards submitted contained the name Jose Manuel OLMOS-
14 Vazquez and a particular date of birth. I searched government databases and identified
15 an individual named Jose Manuel OLMOS-Vazquez who has the same date of birth and
16 resembles the photograph on the fraudulent card. The address on his state-issued driver's
17 license also matches what was provided on the Form I-9.

18 70. One of the cards submitted contained the name [REDACTED]
19 and a particular date of birth. I searched government databases and identified an
20 individual named [REDACTED] who has the same date of birth and
21 resembles the photograph on the fraudulent card. The address on his state-issued driver's
22 license also matches what was provided on the Form I-9.

23 71. One of the cards submitted contained the name Jose Guadalupe
24 PALOMINO-Reyes and a particular date of birth. I searched government databases and
25 identified an individual named Jose Guadalupe PALOMINO-Reyes who has the same
26 date of birth and resembles the photograph on the fraudulent card. The address on his
27 state-issued driver's license also matches what was provided on the Form I-9.

1 72. One of the cards submitted contained the name Jose Andres PEREZ-
2 Rodriguez and a particular date of birth. Along with the fraudulent green card, a
3 Washington driver's license also was submitted in the name of Jose Andres PEREZ-
4 Rodriguez who has the same date of birth and resembles the photograph on the fraudulent
5 card. A search of government databases was conducted, and I determined that the
6 Washington driver's license submitted is authentic with the same name and date of birth
7 presented in the fraudulent document. The address on the driver's license also matches
8 what was provided on the Form I-9.

9 73. One of the cards submitted contained the name [REDACTED]
10 and a particular date of birth. I searched government databases and identified an
11 individual named [REDACTED] who has the same date of birth; however, no
12 photograph exists for his state-issued driver's license because it is suspended/revoked.
13 The address on the driver's license matches what was provided on the Form I-9.

14 74. One of the cards submitted contained the name Benigno R. ALEMAN and
15 a particular date of birth. I searched government databases and identified an individual
16 named Benigno RAYO-Aleman who has the same date of birth. Due to the poor image
17 quality on the fraudulent document, I am unable to determine if the photograph on the
18 fraudulent document matches the one on his state-issued driver's license.

19 75. One of the cards submitted contained the name [REDACTED] and
20 a particular date of birth. I searched government databases and identified an individual
21 named [REDACTED] who has the same date of birth and resembles the
22 photograph on the fraudulent card. The address on his state-issued driver's license also
23 matches what was provided on the Form I-9.

24 76. One of the cards submitted contained the name Jose Mario REGALADO
25 and a particular date of birth. I searched government databases and identified an
26 individual named Jose Mario PEREZ-Regalado who has the same date of birth and
27 resembles the photograph on the fraudulent card.

1 77. One of the cards submitted contained the name Eduardo ROMERO-
2 Gonzalez and a particular date of birth. I searched government databases and identified
3 an individual named Eduardo ROMERO-Gonzalez who has the same date of birth and
4 resembles the photograph on the fraudulent card. The address on his state-issued driver's
5 license also matches what was provided on the Form I-9.

6 78. One of the cards submitted was unable to be read due to the poor quality of
7 the photocopy contained with the Form I-9; however, it is clearly a green card. The
8 information on the Form I-9 associated with that card contained the name Jose Manuel
9 SANCHEZ-Juarez and a particular date of birth. I searched government databases and
10 identified an individual named Jose Manuel SANCHEZ-Juarez who has the same date of
11 birth and, while I could not make out the biographical data on the fraudulent card, I could
12 tell that the photograph on his state-issued driver's license resembles the photograph on
13 the fraudulent card.

14 79. One of the cards submitted contained the name [REDACTED]
15 [REDACTED] and a particular date of birth. I searched government databases and identified an
16 individual named [REDACTED] who has the same date of birth and
17 resembles the photograph on the fraudulent card. The address on his state-issued driver's
18 license also matches what was provided on the Form I-9.

19 80. One of the cards submitted contained the name [REDACTED]
20 [REDACTED] and a particular date of birth. I searched government
21 databases and identified an individual named [REDACTED] who has
22 the same date of birth and resembles the photograph on the fraudulent card. The address
23 on his state-issued driver's license also matches what was provided on the Form I-9.

24 81. One of the cards submitted contained the name Joel VASQUEZ-Ventura
25 and a particular date of birth. I searched government databases and identified an
26 individual named Joel VASQUEZ-Ventura who has the same date of birth and resembles
27 the photograph on the fraudulent card.

82. For all of the individuals listed in paragraphs 34 through 81, immigration records confirm that none of the individuals had lawful permanent resident status and did not have valid work authorization.

83. For the individuals listed below, HSI was not able to associate a true identity with the fraudulent green card. However, I was able to confirm that the cards submitted were in fact fraudulent because the cards contained an A-number that did not match the person's name according to immigration records. In my training and experience, it is highly likely that these individuals are illegally in the United States without valid work authorization because otherwise there would be no need to submit a fraudulent green card during the Form I-9 process.

- a. Eduardo Juarez-Juarez, DOB: [REDACTED]
- b. [REDACTED] DOB: [REDACTED]
- c. Alvaro Rolando Mejia-Ajtum, DOB: [REDACTED]
- d. [REDACTED], DOB: [REDACTED]
- e. Gregorio Quiahua-Medrano, DOB: [REDACTED]
- f. Luis Raymundo, DOB: [REDACTED]
- g. Fredy Orlando Suchite-Campos, DOB: [REDACTED]

C. False Attestations of U.S. Citizenship

84. The next group of individuals certified themselves as United States citizens, which means that they were not required to list an A-number. However, HSI was able to determine that these individuals were not U.S. citizens because the information listed was not accurate, and HSI was able to use reasonably similar biographical information and photographs on the documents provided to determine their likely true identity and immigration history. A search for these individuals revealed no pending applications or petitions that would allow them to legally enter into or remain in the United States.

- a. Juan Manuel LOPEZ-Melgoza, with an associated date of birth of [REDACTED] presented a Washington state driver's license and a Social Security card as proof of United States citizenship. Record checks run on the Social Security number provided revealed that the number does not belong to him. Additional record checks revealed that LOPEZ-

Melgoza is a citizen of Mexico with no A-number issued, who was granted four voluntary returns to Mexico in 2021 and 2022.

- b. David NUNEZ-Hernandez, with an associated date of birth of [REDACTED], presented a Washington state driver's license and a Social Security card as proof of United States citizenship. The I-9 also listed an A-number that does not belong to him. Record checks revealed that NUNEZ-Hernandez is a citizen of Mexico with no A-number issued, who had been previously granted five voluntary returns to Mexico.

D. Surveillance

85. On March 12, 2025, at approximately 6:30 a.m., I initiated surveillance near Mt. Baker Roofing. I observed a number of employees arriving between 6:45 a.m. and 7:10 a.m. I then observed employees departing from the business in Mt. Baker Roofing trucks, presumably to various job sites.⁴ In days thereafter, I was able to gather license plates from the business at various times of the day. During these times, I observed the same vehicles at multiple times of the day, which indicates to me that the occupants of these vehicles are employed at Mt. Baker Roofing. At approximately 6:30 a.m., prior to most employees arriving, I have not observed more than four vehicles in the parking lot. In the days I have conducted surveillance, over the next 45 minutes as employees arrive and throughout the day, I have observed as many as 45-50 vehicles that appear to be personally-owned vehicles, not associated with the company, parked in the lot.

86. Of particular interest, I have observed ten Washington-plated vehicles registered to individuals discussed earlier in this affidavit who have used fraudulent identity documents to gain employment at Mt. Baker Roofing.

87. On March 19, 2025 and March 21, 2025, HSI Group Supervisor (GS) [REDACTED] long with Customs and Border Protection Office Air and Marine

⁴ In order to be covert, I did not observe the activity inside the parking lot and around the business and only observed vehicles turning onto Thomas Road toward the business and onto Pacific Highway when the Mt. Baker Roofing trucks departed the business.

Operations, conducted aerial surveillance between 6:30 a.m. and 7:45 a.m. On March 19, 2025, GS [REDACTED] observed most of the employees' vehicles arriving between 6:50 a.m. and 7:10 a.m. At approximately 7:15 a.m., the employees gathered for what appeared to be a meeting, which lasted for approximately ten minutes. After the meeting, it appeared that the employees gathered supplies and equipment and loaded up their Mt. Baker Roofing vehicles before leaving the area. On March 21, 2025, while the times of arrival were approximately the same, there was no meeting. and the employees were more loosely setting up their trucks and leaving the business. Based on the times observed during multiple surveillance operations, agents expect to execute this search warrant in the morning before employees leave the business premises.

E. Training and Experience

88. One of the things that I seek to seize are any identification cards for the individuals associated with the fraudulent green cards. Based on my training and experience, I know that individuals carry identification documents on their person, such as in their wallets. I know that Section 264(e) of the INA requires permanent residents to carry their green cards with them at all times, although I know that individuals who use fraudulent identification do not always do so. Identification documents will be important evidence. If individuals possess any of the fraudulent identification documents that were submitted during the Form I-9 process, then that will tie them personally to the false submissions. If individuals possess any valid identification, that will help show that the fraudulent green cards are in fact fraudulent by establishing their true identity.⁵

89. I know that it is common in the United States for aliens without legal work authorization to submit fraudulent identity documents in order to obtain employment.

⁵ On February 10, 2025, ICE civilly arrested Dionancio Lopez-Lopez for being present unlawfully in the United States. Lopez-Lopez worked for Mt. Baker Roofing until his termination on February 14, 2025. Mr. Baker Roofing produced a green card for Lopez-Lopez as part of its I-9 Form production. The green card was fraudulent. The arresting officers do not recall Lopez-Lopez having the fraudulent card on him at the time of arrest.

1 90. I know that some U.S. employers disregard employment verification
2 processes for the purposes of exploiting labor for financial advantage. In particular, I
3 know in my training and experience that certain employers will hire individuals with
4 illegal work status because employers can pay these individuals a lower wage. In
5 addition, workers without legal status are less likely to complain about working
6 conditions because they do not want to draw attention to themselves, given their
7 immigration status. I know in this case that, as described above, the fraudulent nature of
8 some of the green cards would have been apparent to anyone who examined them with
9 any care.

10 91. I know from training and experience that employers who hire aliens
11 without valid work authorization for the purpose of cheaper labor often will conceal their
12 illegal hiring practices by requesting that their applicants supply employment eligibility
13 documents and identity documents, but will knowingly accept fraudulent and/or
14 counterfeit documentation in order to nominally satisfy the Form I-9 reporting
15 requirements.

16 92. I know based on my training and experience that a business, such as Mt.
17 Baker Roofing, is likely to retain payroll and other records showing who worked at the
18 business, for what period of time, and how much individuals were paid. These materials
19 would be important to establishing the crimes identified above, given the need to show
20 that any given unauthorized worker did in fact work at the business.

21 93. On March 17, 2025, Mt. Baker Roofing provided me, via email, documents
22 requested via administrative subpoena as part of the I-9 inspection process. The
23 documents that were provided included basic payroll data, an employee roster (which
24 shows the name, date of birth, Social Security number, address, and dates of
25 hire/termination), and basic documents about the business that can be found in open-
26 source searches. Only basic information was requested by subpoena and based on my
27

1 training and experience, additional, more detailed employee and payroll information, not
2 previously provided, will be found at the business.

4 MANNER OF EXECUTION

5 94. As set forth above, HSI intends to execute this warrant at a time when
6 workers are believed to gather in the morning at the work premises described in
7 Attachment A-1. HSI intends to detain the employees present at the premises to
8 minimize the risk of harm to officers, to ensure the orderly completion of the search, to
9 minimize the risk of flight, and for the purpose of determining whether any of the
10 employees are any of the individuals described in Attachment A-2, *i.e.*, any individuals
11 associated with the fraudulent green cards and other false Form I-9 submissions. In order
12 to determine if any of the individuals encountered are in fact an individual described in
13 Attachment A-2, agents plan to ask the individuals their name and to fingerprint them, if
14 necessary. Agents plan to take these steps to ensure that they are searching the correct
15 individuals, given that the fraudulent green card photographs are of uneven quality, and
16 that often individuals look different compared to their identification photographs.

17 95. HSI plans to arrest civilly any individuals listed on Attachment A-2 who
18 they identify and process them for immigration violations. HSI will also, in its
19 discretion, make any appropriate criminal referrals to the United States Attorney's Office
20 for offenses committed by the employer and/or the employees. As reflected in
21 Attachment B-1, HSI also will search the business for employment records and
22 associated items and otherwise attempt to conduct interviews in furtherance of the crimes
23 listed in the warrant.

25 COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

26 96. As described above and in Attachment B, this application seeks permission
27 to search for evidence that might be found at the business, in whatever form it is found.

1 One form in which the evidence might be found is data stored on computer hard drives or
2 other electronic storage media. Thus, the warrant applied for would authorize the seizure
3 of computers or other electronic storage media or, potentially, the copying of
4 electronically stored information from computers or other electronic storage media, all
5 under Rule 41(e)(2)(B).

6 97. *Probable cause.* Based upon my review of the evidence gathered in this
7 investigation, my review of data and records, information received from other agents and
8 computer forensics examiners, and my training and experience, I submit that if a
9 computer or other electronic storage media is found at the business, there is probable
10 cause to believe that evidence of the crimes identified above will be stored on those
11 computers or other electronic storage media. I believe computers or other electronic
12 storage media likely contain payroll and other employment records relevant to the
13 employees listed in Attachment A-2. There is, therefore, probable cause to believe that
14 evidence of the crimes identified above exists and will be found on computers or other
15 electronic storage media at the business, for at least the following reasons:

- 16
- 17 a. Based on my knowledge, training, and experience, I know that computer
18 files or remnants of such files can be preserved (and consequently also then
19 recovered) for months or even years after they have been downloaded onto
20 a storage medium, deleted, or accessed or viewed via the Internet.
21 Electronic files downloaded to a digital device or other electronic storage
22 medium can be stored for years at little or no cost. Even when files have
23 been deleted, they can be recovered months or years later using forensic
24 tools. This is so because when a person “deletes” a file on a digital device
25 or other electronic storage media, the data contained in the file does not
26 actually disappear; rather, that data remains on the storage medium until it
27 is overwritten by new data.
- 24 b. Therefore, deleted files, or remnants of deleted files, may reside in free
25 space or slack space—that is, in space on the digital device or other
26 electronic storage medium that is not currently being used by an active
27 file—for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
- e. I also know that businesses often include payroll and employment records for extended periods of time for tax and other reasons.

98. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computers or other electronic storage media located at the business because:

- a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

1 b. As explained herein, information stored within a computer and other
2 electronic storage media may provide crucial evidence of the “who, what, why,
3 when, where, and how” of the criminal conduct under investigation, thus
4 enabling the United States to establish and prove each element or alternatively,
5 to exclude the innocent from further suspicion. In my training and experience,
6 information stored within a computer or storage media (e.g., registry
7 information, communications, images and movies, transactional information,
8 records of session times and durations, internet history, and anti-virus,
9 spyware, and malware detection programs) can indicate who has used or
10 controlled the computer or storage media. This “user attribution” evidence is
11 analogous to the search for “indicia of occupancy” while executing a search
12 warrant at a residence. The existence or absence of anti-virus, spyware, and
13 malware detection programs may indicate whether the computer was remotely
14 accessed, thus inculcating or exculpating the computer owner and/or others
15 with direct physical access to the computer. Further, computer and storage
16 media activity can indicate how and when the computer or storage media was
17 accessed or used. For example, as described herein, computers typically
18 contain information that log: computer user account session times and
19 durations, computer activity associated with user accounts, electronic storage
20 media that connected with the computer, and the IP addresses through which
21 the computer accessed networks and the internet. Such information allows
22 investigators to understand the chronological context of computer or electronic
23 storage media access, use, and events relating to the crime under investigation.
24 Additionally, some information stored within a computer or electronic storage
25 media may provide crucial evidence relating to the physical location of other
26 evidence and the suspect. For example, images stored on a computer may both
27 show a particular location and have geolocation information incorporated into
its file data. Such file data typically also contains information indicating when
the file or image was created. The existence of such image files, along with
external device connection logs, may also indicate the presence of additional
electronic storage media (e.g., a digital camera or cellular phone with an
incorporated camera). The geographic and timeline information described
herein may either inculcate or exculpate the computer user. Last, information
stored within a computer may provide relevant insight into the computer user’s
state of mind as it relates to the offense under investigation. For example,
information within the computer may indicate the owner’s motive and intent to
commit a crime (e.g., internet searches indicating criminal planning), or
consciousness of guilt (e.g., running a “wiping” program to destroy evidence
on the computer or password protecting/encrypting such evidence in an effort
to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer or other
electronic storage media works can, after examining this forensic evidence in

1 its proper context, draw conclusions about how the digital device or other
2 electronic storage media were used, the purpose of their use, who used them,
3 and when.

4 d. The process of identifying the exact files, blocks, registry entries, logs, or
5 other forms of forensic evidence on a digital device or other electronic storage
6 media that are necessary to draw an accurate conclusion is a dynamic process.
7 While it is possible to specify in advance the records to be sought, digital
8 evidence is not always data that can be merely reviewed by a review team and
9 passed along to investigators. Whether data stored on a computer is evidence
10 may depend on other information stored on the computer and the application of
11 knowledge about how a computer behaves. Therefore, contextual information
12 necessary to understand other evidence also falls within the scope of the
13 warrant.

14 e. Further, in finding evidence of how a computer or other electronic storage
15 media was used, the purpose of its use, who used it, and when, sometimes it is
16 necessary to establish that a particular thing is not present. For example, the
17 presence or absence of counter-forensic programs or anti-virus programs (and
18 associated data) may be relevant to establishing the user's intent.

19 **PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION**

20 99. As set forth above, I previously served an administrative record for
21 materials from the business. Attachment B-1 seeks material that is broader than what
22 was sought under the subpoena. Although I am not aware of the business withholding
23 any documents that were covered by the subpoena, I nonetheless have concerns whether
24 the business would fully produce all of the documents I am now seeking, given the
25 business will understand with the execution of the search warrant that its conduct is being
26 investigated.

27 **COMPUTERS**

100. *Necessity of seizing or copying entire computers or storage media.* In most
cases, a thorough search of premises for information that might be stored on digital
devices or other electronic storage media often requires the seizure of the physical items

1 and later off-site review consistent with the warrant. In lieu of removing all of these
2 items from the premises, it is sometimes possible to make an image copy of the data on
3 the digital devices or other electronic storage media, onsite. Generally speaking, imaging
4 is the taking of a complete electronic picture of the device's data, including all hidden
5 sectors and deleted files. Either seizure or imaging is often necessary to ensure the
6 accuracy and completeness of data recorded on the item, and to prevent the loss of the
7 data either from accidental or intentional destruction. This is true because of the
8 following:

9 a. *The time required for an examination.* As noted above, not all evidence
10 takes the form of documents and files that can be easily viewed on site.
11 Analyzing evidence of how a computer has been used, what it has been used
12 for, and who has used it requires considerable time, and taking that much time
13 on premises could be unreasonable. As explained above, because the warrant
14 calls for forensic electronic evidence, it is exceedingly likely that it will be
15 necessary to thoroughly examine the respective digital device and/or electronic
16 storage media to obtain evidence. Computer hard drives, digital devices and
17 electronic storage media can store a large volume of information. Reviewing
18 that information for things described in the warrant can take weeks or months,
19 depending on the volume of data stored, and would be impractical and invasive
20 to attempt on-site.

21 b. *Technical requirements.* Digital devices or other electronic storage media
22 can be configured in several different ways, featuring a variety of different
23 operating systems, application software, and configurations. Therefore,
24 searching them sometimes requires tools or knowledge that might not be
25 present on the search site. The vast array of computer hardware and software
26 available makes it difficult to know before a search what tools or knowledge
27 will be required to analyze the system and its data on the premises. However,
taking the items off-site and reviewing them in a controlled environment will
allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant
could be stored in a variety of electronic storage media formats and on a
variety of digital devices that may require off-site reviewing with specialized
forensic tools.

SEARCH TECHNIQUES

101. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying computers or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

102. The business to be searched is a functioning company that conducts legitimate business. The seizure of the business's computers may limit the business's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the business so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the business's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

103. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

B. Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to

1 determine if it is possible to secure the data contained on these devices onsite
2 in a reasonable amount of time and without jeopardizing the ability to
accurately preserve the data.

3 b. In order to examine the electronically stored information (“ESI”) in a
4 forensically sound manner, law enforcement personnel with appropriate
5 expertise will attempt to produce a complete forensic image, if possible and
6 appropriate, of any digital device or other electronic storage media that is
capable of containing data or items that fall within the scope of Attachment B
to this Affidavit.¹

7 c. A forensic image may be created of either a physical drive or a logical
8 drive. A physical drive is the actual physical hard drive that may be found in a
9 typical computer. When law enforcement creates a forensic image of a
10 physical drive, the image will contain every bit and byte on the physical drive.
11 A logical drive, also known as a partition, is a dedicated area on a physical
12 drive that may have a drive letter assigned (for example the c: and d: drives on
a computer that actually contains only one physical hard drive). Therefore,
13 creating an image of a logical drive does not include every bit and byte on the
14 physical drive. Law enforcement will only create an image of physical or
15 logical drives physically present on or within the subject device. Creating an
16 image of the devices located at the search locations described in Attachment A
will not result in access to any data physically located elsewhere. However,
17 digital devices or other electronic storage media at the search locations
described in Attachment A that have previously connected to devices at other
locations may contain data from those other locations.

18 d. If based on their training and experience, and the resources available to
19 them at the search site, the search team determines it is not practical to make an
on-site image within a reasonable amount of time and without jeopardizing the
20 ability to accurately preserve the data, then the digital devices or other

21
22 ¹ The purpose of using specially trained computer forensic examiners to conduct the
23 imaging of digital devices or other electronic storage media is to ensure the integrity of
the evidence and to follow proper, forensically sound, scientific procedures. When the
24 investigative agent is a trained computer forensic examiner, it is not always necessary to
separate these duties. Computer forensic examiners often work closely with investigative
25 personnel to assist investigators in their search for digital evidence. Computer forensic
examiners are needed because they generally have technological expertise that
26 investigative agents do not possess. Computer forensic examiners, however, often lack
the factual and investigative expertise that an investigative agent may possess on any
27 given case. Therefore, it is often important that computer forensic examiners and
investigative personnel work closely together.

1 electronic storage media will be seized and transported to an appropriate law
2 enforcement laboratory to be forensically imaged and reviewed.

3 **C. Searching the Forensic Images.**

4 a. Searching the forensic images for the items described in Attachment B may
5 require a range of data analysis techniques. In some cases, it is possible for
6 agents and analysts to conduct carefully targeted searches that can locate
7 evidence without requiring a time-consuming manual search through unrelated
8 materials that may be commingled with criminal evidence. In other cases,
9 however, such techniques may not yield the evidence described in the warrant,
10 and law enforcement may need to conduct more extensive searches to locate
11 evidence that falls within the scope of the warrant. The search techniques that
12 will be used will be only those methodologies, techniques and protocols as
13 may reasonably be expected to find, identify, segregate and/or duplicate the
14 items authorized to be seized pursuant to Attachment B to this affidavit. Those
15 techniques, however, may necessarily expose many or all parts of a hard drive
16 to human inspection in order to determine whether it contains evidence
17 described by the warrant.

18 b. These methodologies, techniques and protocols may include the use of a
19 “hash value” library to exclude normal operating system files that do not need
20 to be further searched. However, because the evidence I am seeking does not
21 have particular known hash values, agents will not be able to use any type of
22 hash value library to locate the items identified in Attachment B.
23
24
25
26
27

CONCLUSION

104. Based on foregoing, I seek authorization to search the areas specified in Attachments A for the items specified in Attachments B. Attachment A-1 describes the Mt. Baker Roofing business to be searched, and Attachment B-1 are the items I seek to seize from the business. Attachment A-2 contains depictions of the fraudulent green cards described above. It also contains the true identities associated with the cards, and the other fraudulent submissions, as described above. I seek authorization to search any of the individuals depicted in the cards or who match the true identities set forth in Attachment A-2. Attachment B-2 are the items I seek to seize from the individuals.

Special Agent
Homeland Security Investigations

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 25th day of March, 2025.


BRIAN A. TSUCHIDA
United States Magistrate Judge

ATTACHMENT A-1

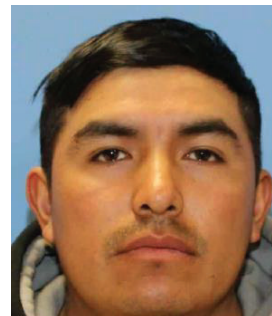
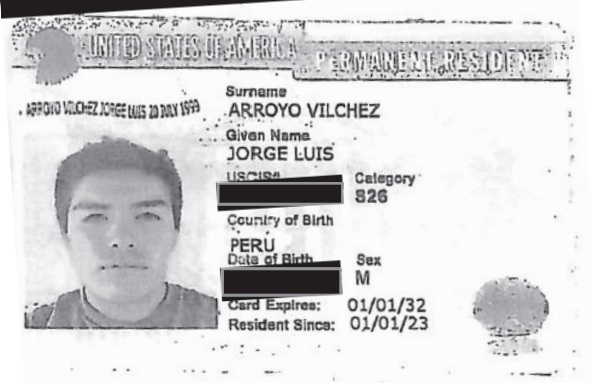
Property to Be Searched

The property, located at 928 Thomas Road, Bellingham, WA 98226, is described as a set of one-story buildings and trailers, with grey metal siding and white metal roofs. Two additional trailers in the rear of the property are light-colored with grey roofs. Surrounding the buildings are numerous parking areas. The first building on the left while driving eastbound on Thomas Road is embossed with the logo for Mt. Baker Roofing. This authorization is being requested for the structures on the premises of the business and any business vehicles.



ATTACHMENT A-2

People to Be Searched



3. Heriberto AYALA-Gonzalez, DOB: [REDACTED], WA DL:





5. Marco Antonio CISNEROS-Palomino, DOB: [REDACTED], MXN Passport:

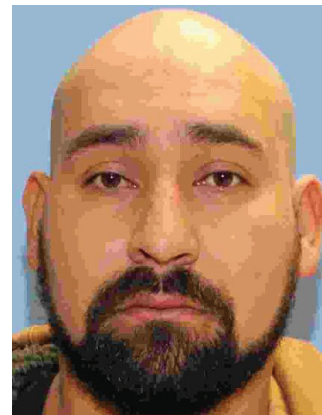
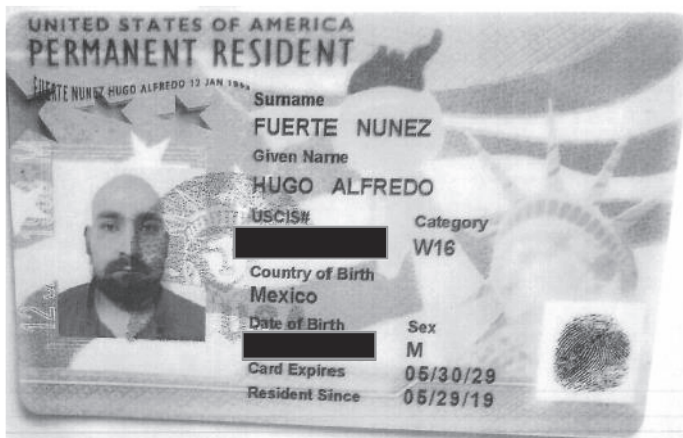


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27





11. Hugo Alfredo FUERTE-Nunez, DOB: [REDACTED] WA DL:

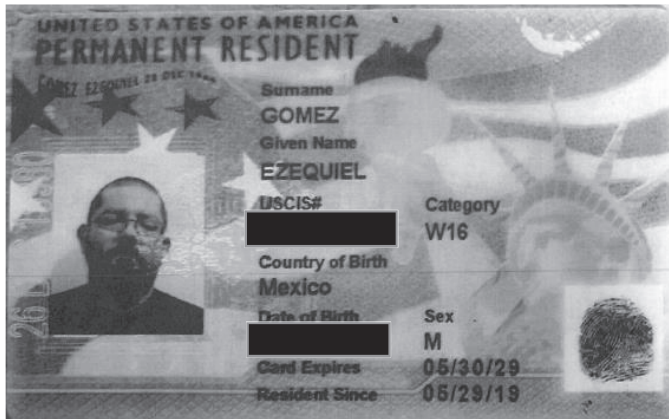


Attachment A-2

USAO # 2025R00399

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

13. Ezequiel GOMEZ-Cruz, DOB: [REDACTED], WA DL: [REDACTED]



14. Santos GONALEZ-Feliciano, DOB: [REDACTED], WA DL: [REDACTED]



15. Diego GONZALEZ-Rosas, DOB: [REDACTED], WA DL: [REDACTED]



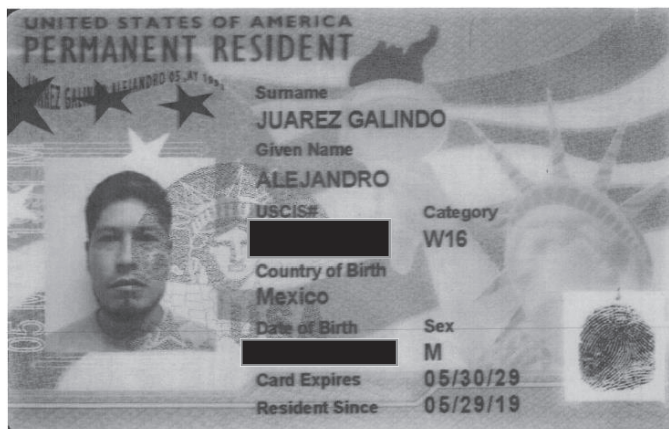
16. Frank Brayan GUTIERREZ-Gutierrez, DOB: [REDACTED], WA DL: [REDACTED]



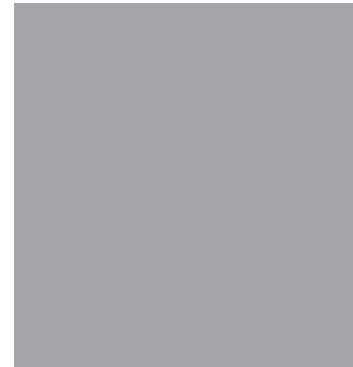
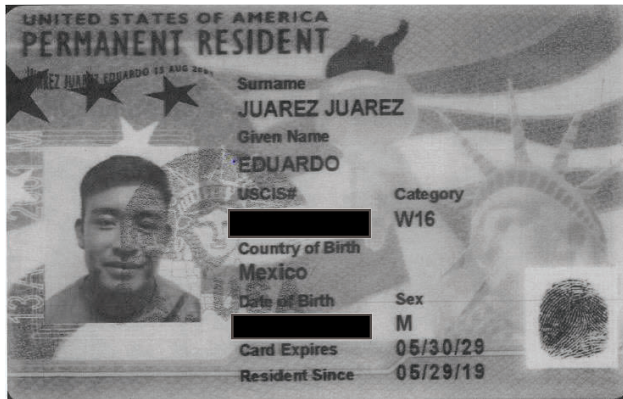
17. Iran HURTADO-Cancino, DOB: [REDACTED], WA DL: [REDACTED]



18. Alejandro JUAREZ-Galindo, DOB: [REDACTED] (I-9) or [REDACTED] (WA DL),
WA DL: [REDACTED]



19. Eduardo JUAREZ-Juarez, DOB: [REDACTED] No WA Driver's License Found

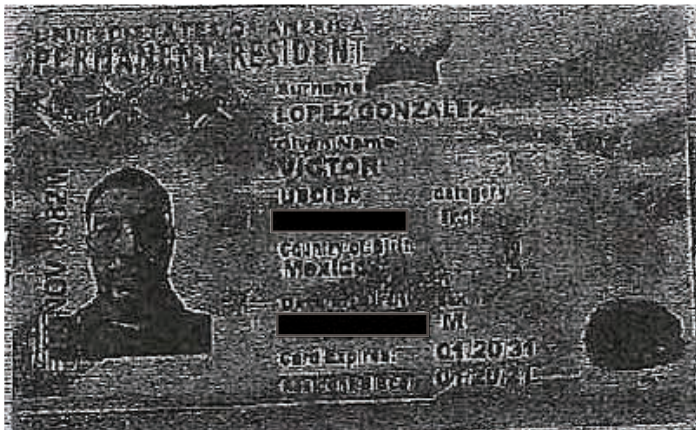




23. Joaquin JUAREZ-Ortiz DOB: [REDACTED], WA DL: [REDACTED]



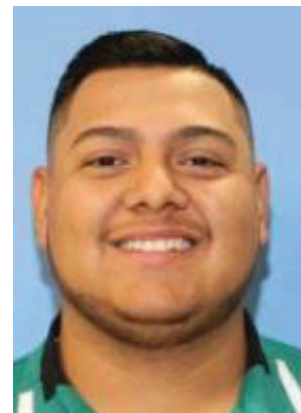
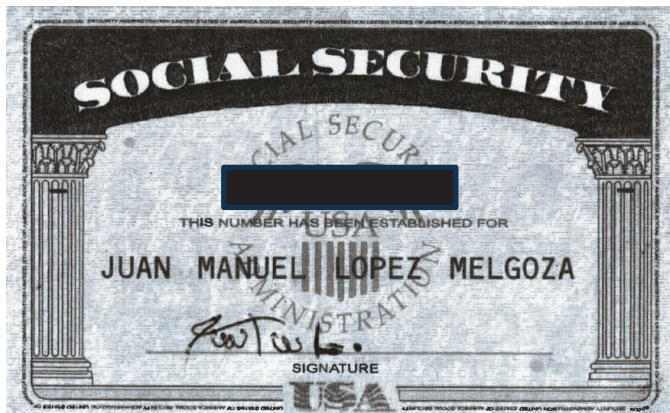
24. Victor LOPEZ-Gonzalez, DOB: [REDACTED], WA DL: [REDACTED]



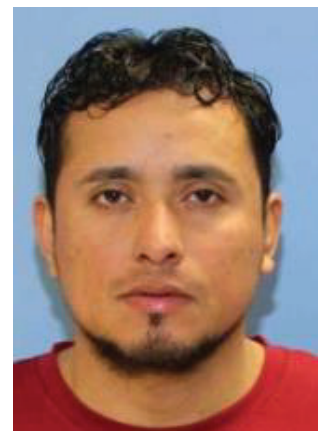
25. Alberino LOPEZ-Cruz, DOB: [REDACTED], WA DL: [REDACTED]



26. Juan Manuel LOPEZ-Melgoza, DOB: [REDACTED], WA DL: [REDACTED], Claimed to be United States Citizen



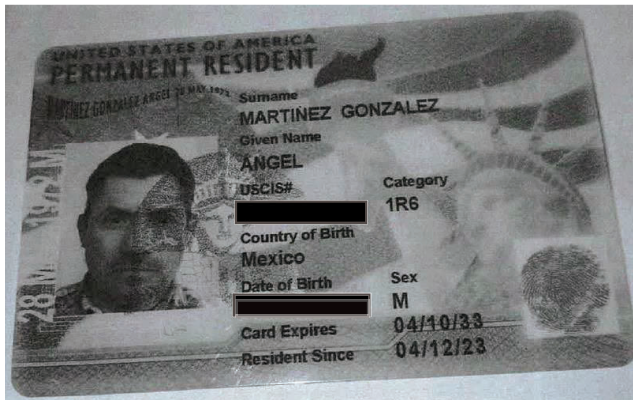
27. Elder Edgardo MANCIA-Ramirez, DOB: [REDACTED] WA DL: [REDACTED]



28. Omar MARILES-Valencia, DOB: [REDACTED], WA DL: [REDACTED]



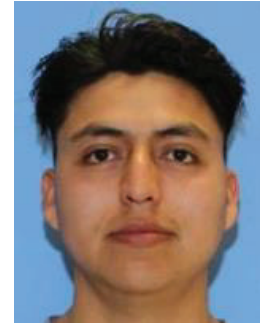
29. Angel MARTINEZ-Gonzalez, DOB: [REDACTED], WA DL: [REDACTED]



30. Luis Mario MARTINEZ-Ortela, DOB: [REDACTED], WA DL: [REDACTED]



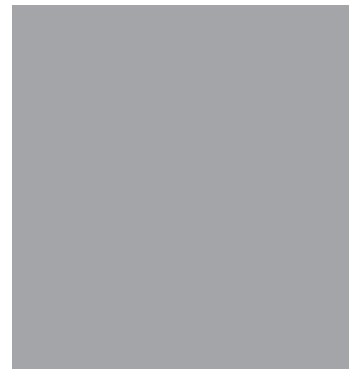
31. Rogelio MARTINEZ-Ortela, DOB: [REDACTED] WA DL: [REDACTED]



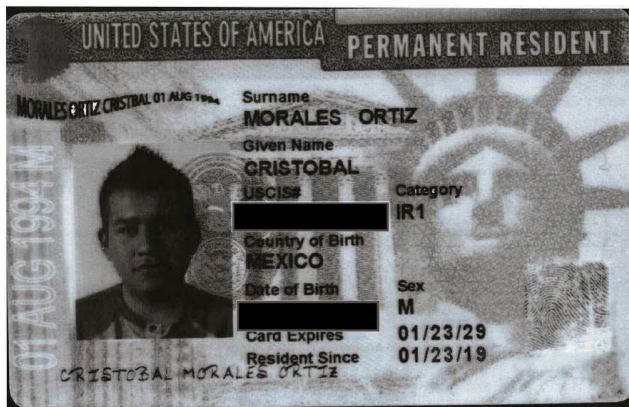
32. Jose Manuel MATEO, DOB: [REDACTED] WA DL: [REDACTED]



33. Alvaro Rolando MEJIA-Ajtum, DOB: [REDACTED], No WA DL Found

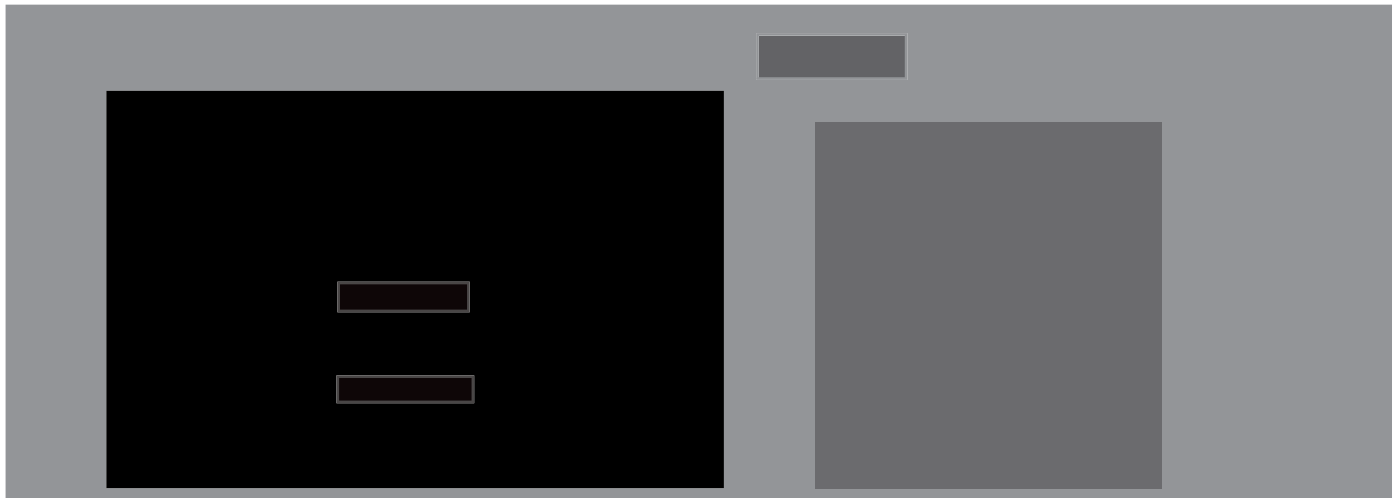


34. Cristobal MORALES-Ortiz, DOB: [REDACTED], WA DL: [REDACTED]

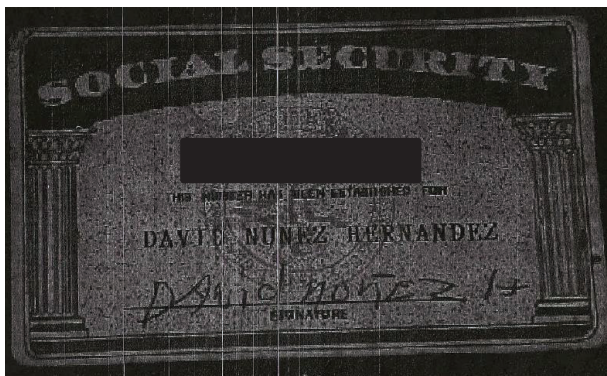


35. Jesus Abelardo MORELOS-Cuevas, DOB: [REDACTED] WA DL: [REDACTED]





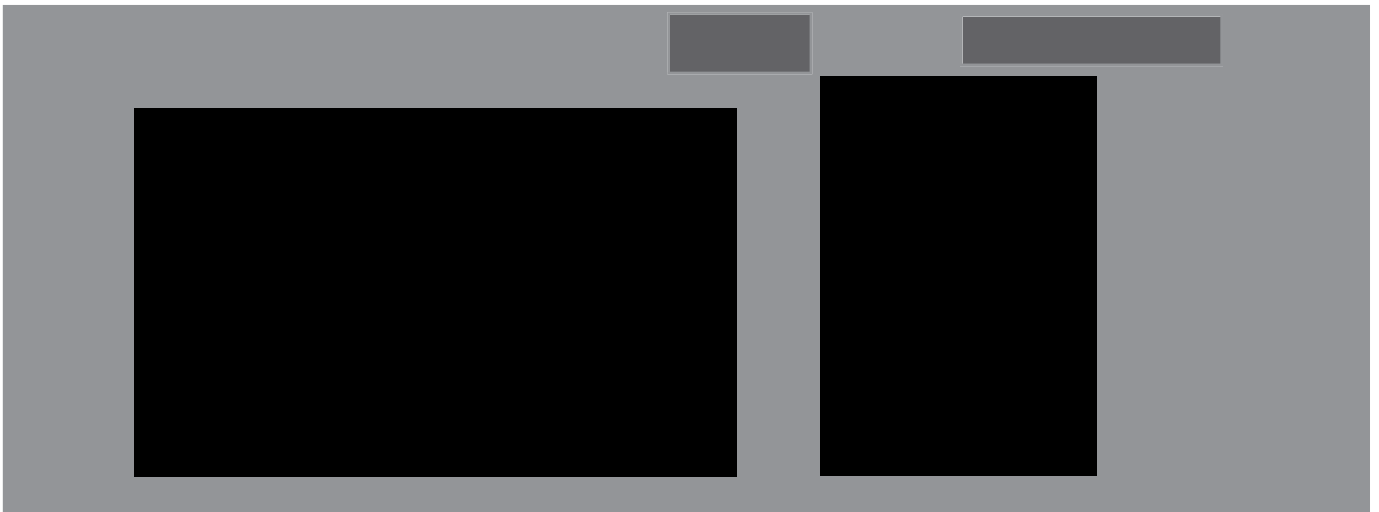
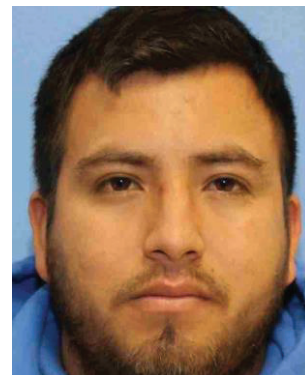
39. David NUNEZ-Hernandez, DOB: [REDACTED] WA DL: [REDACTED],
Claims to be a United States Citizen



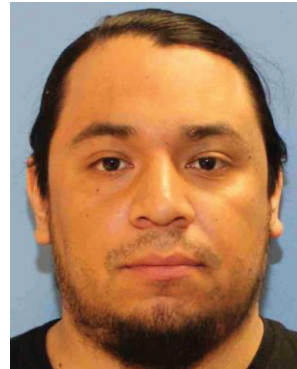
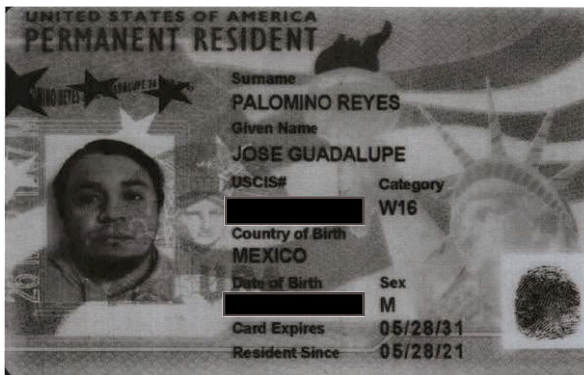
40. Edgar OLMOS-Vazquez, DOB: [REDACTED], WA DL: [REDACTED]



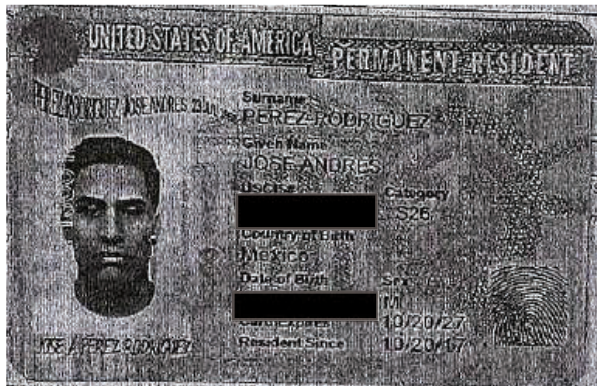
41. Jose Manuel OLMOS-Vazquez, DOB: [REDACTED], WA DL: [REDACTED]



43. Jose Guadalupe PALOMINO-Reyes, DOB: [REDACTED] WA DL: [REDACTED]



44. Jose Andres PEREZ-Rodriguez, DOB: [REDACTED] WA DL: [REDACTED]

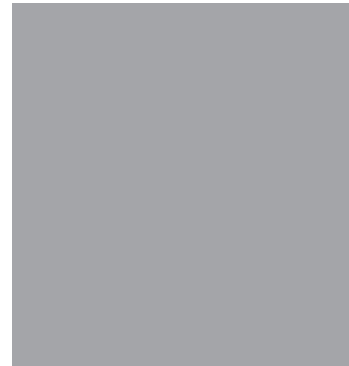


45. Gregorio Quiahua Medrano, DOB: [REDACTED], No WA Driver's License Found

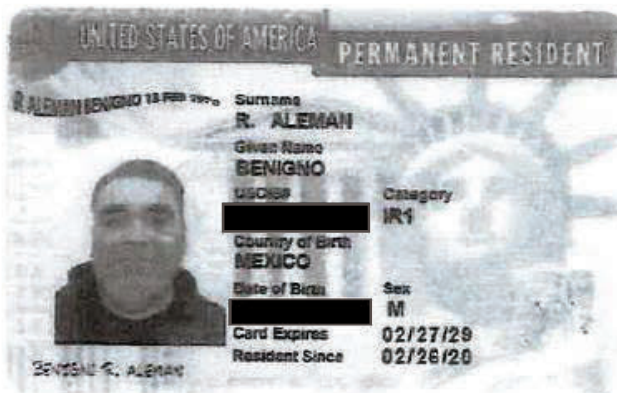




47. Luis Raymundo, DOB: [REDACTED], No WA Driver's License Found

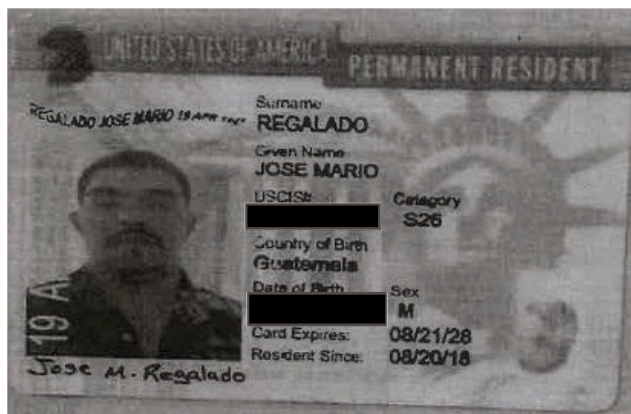


48. Benigno RAYO-Aleman, DOB: [REDACTED] WA DL: [REDACTED]

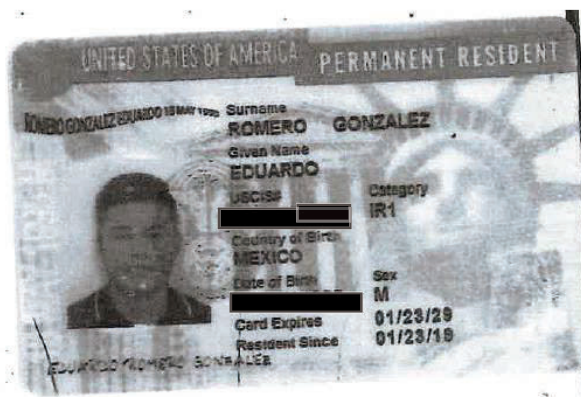




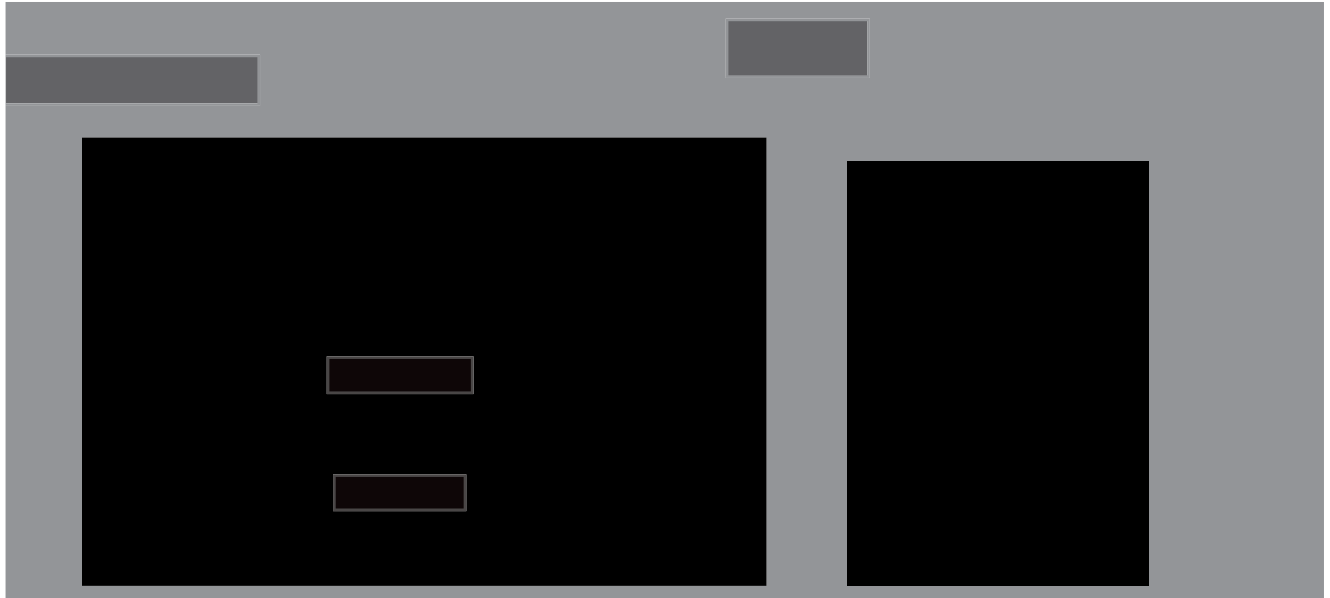
50. Jose Mario PEREZ-Regalado, DOB: [REDACTED], WA DL:



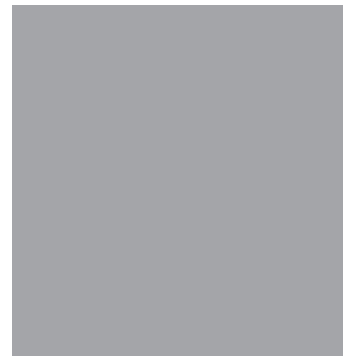
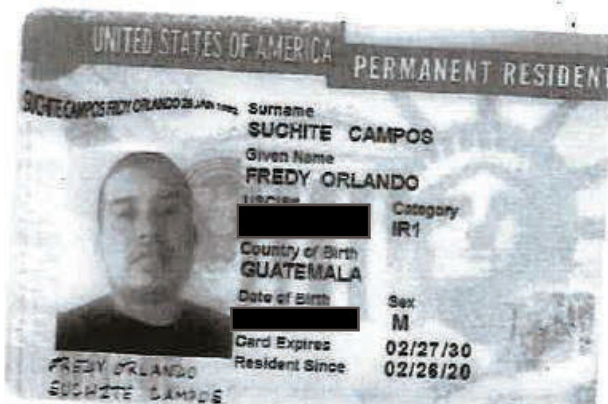
51. Eduardo ROMERO-Gonzalez, DOB: [REDACTED], WA DL:

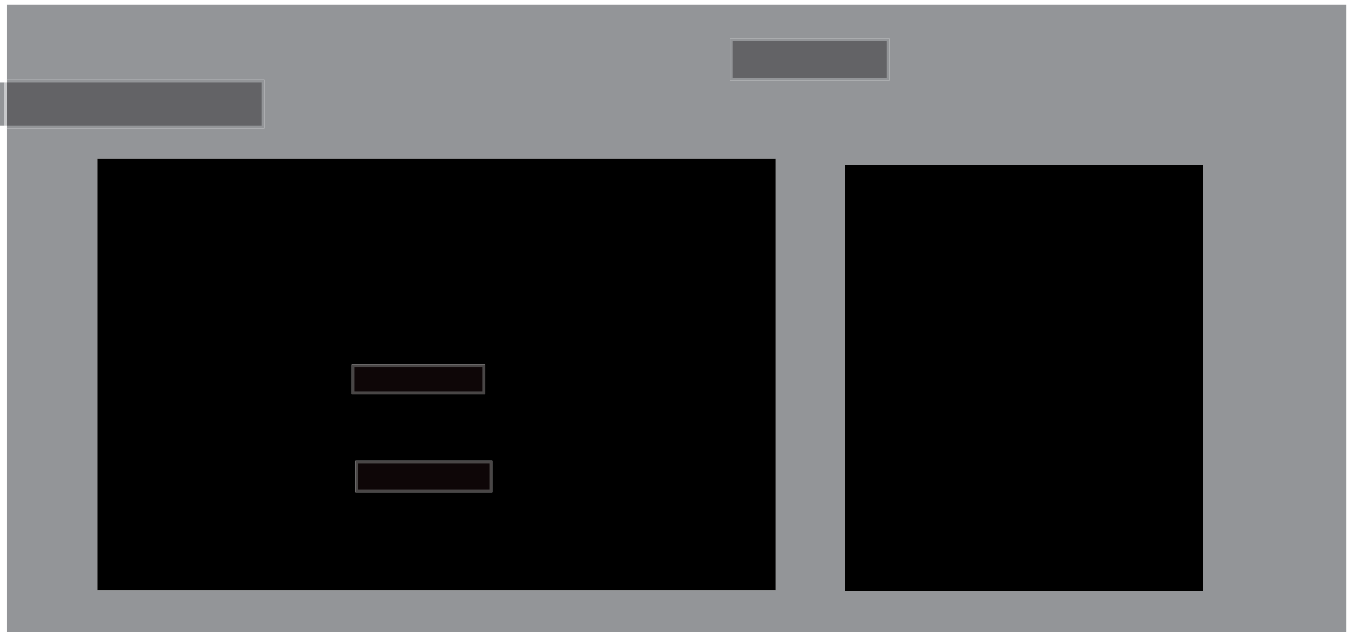


52. Jose Manuel SANCHEZ Juarez, DOB: [REDACTED], WA DL:



54. Fredy Orlando SUCHITE-Campos, DOB: [REDACTED], No WA Driver's License Found





56. Joel VASQUEZ-Ventura, DOB: [REDACTED], WA DL: [REDACTED]



ATTACHMENT B-1**Particular Things to be Seized From Location A-1**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 8 U.S.C. § 1324(a); 8 U.S.C. § 1324a; 18 U.S.C. § 1001; 18 U.S.C. § 911; 18 U.S.C. § 1015(e); and 18 U.S.C. § 1546, 42 U.S.C. § 408(a)(7)(B), namely:

1. Employment records for current and former employees, including but not limited to, personnel files, time cards, production cards, payroll information, bank account information, employee work schedules, employment applications, video recordings of employees, photographs of employees, employment verification documents, Social Security Administration Employer Correction Requests (No-Match letters), Social Security Administration Request for Employee Information (No-Match letters), and Department of Homeland Security (DHS) immigration eligibility documents including DHS Forms I-9;

2. Any employee identification documents and immigration documents in any form, to include but not limited to, immigration visas, entry documents, passports, Social Security cards, Form I-551s, employment authorization documents;

3. Any correspondence with government agencies pertaining to employment, such as the Department of Homeland Security, Social Security Administration, and United States Citizenship and Immigration Services;

4. Any documents pertaining to the true identities of the individuals identified in Attachment A-2;

1 5. Documents and records pertaining to the ownership and management of the
2 business;

3 6. Records and information relating to recruiting individuals, hiring
4 individuals, verification of an individual's true identity, and their status to legally work in
5 the United States;

6 7. Communications regarding the use, sourcing, manufacturing, and/or
7 procurement of fraudulent identification documents.

8 8. Computers or other electronic storage media⁶ containing any of the records
9 or information described above or used as a means to commit the violations described
10 above, including to generate, store, or transmit records in furtherance of the violations.

11 9. For any digital device or other electronic storage media upon which
12 electronically stored information that is called for by this warrant may be contained, that
13 may contain things otherwise called for by this warrant, or whose seizure is otherwise
14 authorized by this warrant:

15 a. evidence of who used, owned, or controlled the computer or other
16 electronic storage media at the time the things described in this warrant were created,
17 edited, or deleted, such as logs, registry entries, configuration files, saved usernames and
18 passwords, documents, browsing history, user profiles, email, email contacts, "chat,"
19 instant messaging logs, photographs, and correspondence;

20 b. evidence of software that would allow others to control the digital
21 device or other electronic storage media, such as viruses, Trojan horses, and other forms
22 of malicious software, as well as evidence of the presence or absence of security software
23 designed to detect malicious software;

24 c. evidence of the lack of such malicious software;

25 d. evidence of the attachment to the computer to other storage devices
26 or similar containers for electronic evidence;

27 e. evidence of the times the computer or other electronic storage media
was used;

⁶ Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 f. physical keys, encryption devices, dongles and similar physical
2 items that are necessary to gain access to the computer equipment, storage devices or
3 data; and

4 g. passwords, password files, test keys, encryption codes or other
5 information necessary to access the computer equipment, storage devices or data.

6 h. documentation and manuals that may be necessary to access the
7 digital device or other electronic storage media or to conduct a forensic examination of
8 the digital device or other electronic storage media;

9 i. applications, utility programs, compilers, interpreters, and other
10 software used to facilitate direct or indirect communication with the computer hardware,
11 storage devices, or data to be searched;

12 j. contextual information necessary to understand the evidence
13 described in this attachment.

14 THE SEIZURE OF COMPUTERS OR OTHER ELECTRONIC STORAGE MEDIA
15 AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY
16 AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT
17 THAT SUCH COMPUTERS OR OTHER ELECTRONIC STORAGE MEDIA
18 CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY
19 DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING
20 OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE,
21 INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.
22
23
24
25
26
27

ATTACHMENT B-2

Particular Things to be Seized from the Individuals Identified in A-2

The following records, documents, files, or materials that constitute evidence, instrumentalities, or fruits of violations of 8 U.S.C. § 1324(a); 8 U.S.C. § 1324a; 18 U.S.C. § 1001; 18 U.S.C. § 911; 18 U.S.C. § 1015(e); and 18 U.S.C. § 1546, 42 U.S.C. § 408(a)(7)(B), namely:

1. Identity documents or copies of identity documents, in any form, and whether fraudulent or not, including, but not limited to:
 - a. Form I-551 Permanent Resident Card (“Green Card”);
 - b. Form I-766 Employment Authorization Document Card;
 - c. U.S. and foreign passports;
 - d. Visas;
 - e. I-94 Departure Records;
 - f. birth certificates;
 - g. Social Security cards;
 - h. foreign national identity documents;
 - i. driver’s licenses;
 - j. applications to obtain such documents;
2. Pay stubs or other records reflecting employment at Mt. Baker Roofing.